NIPEC/18/16
(replacing NIPEC/16/16)

NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL
FOR NURSING AND MIDWIFERY

Policy for the reporting of:
Adverse Incidents / Accidents / Near Misses and Dangerous Occurrences

May 2018

Review date: May 2021

Centre House
79 Chichester Street
BELFAST
BT1 4JE
Tel: 0300 300 0066
www.nipec.hscni.net

Contents

1. INTRODUCTION

1.1 This document sets out the NIPEC policy for the reporting of incidents and gives guidance on what staff should do following an incident, how it should be managed and investigated. It encourages a reporting and learning culture with safety at its heart.

1.2 The policy has been developed in line with the BSO policy which involved consultation with representatives from the Health & Safety Committee, Human Resources, Trade Unions and the Equality Unit and took account of HSCB/DoH requirements.

1.3 Reporting all data breaches, accidents and near misses, however trivial they may appear enables a profile to be built of the risks to staff, visitors and the business of NIPEC, from which a strong and factual basis for targeting resources effectively can be developed. By understanding the patterns and trends of incidents, NIPEC is better placed to manage the underlying risks.

1.4 NIPEC supports a culture of safety and openness. All staff are required to report incidents, accidents, near misses and potential incidents so that steps can be taken to improve the safety of visitors and staff. This awareness may serve to alert management and other staff to areas of potential risk at an early stage and enable avoiding action to be taken by improving work practice, and through feedback and learning provide a valuable source of learning and improvement.

2. RESPONSIBILITIES

2.1 The **NIPEC Council** has overall responsibility for effective risk management and this includes oversight of the management of adverse incidents within NIPEC for which the Chief Executive is accountable. The Head of Corporate Services has operational responsibility of this policy and is supported by the Corporate Services Manager in the day to day administration of the process.

2.2 The **Business Team** is responsible for:

- Seeking assurance and advising the Council on the management of serious adverse incidents.

2.3 **Managers** are responsible for implementing the policy by:

- Ensuring that all staff are aware of the policy and procedures.
- Ensuring appropriate and timely reporting of incidents.
- Working with the Corporate Services Manager and other local staff who have responsibility for health and safety and/or information management.
- Supporting the reporting process of reviewing and investigating local incidents.

- Taking local remedial and preventative action and informing NIPEC's Health & Safety Committee and Information Governance Group of such action and about any lessons learned.
- Supporting and debriefing staff.

2.4 The **Head of Corporate Services**, assisted by the **Corporate Services Manager**, will**:**

- Ensure accessibility of up to date reporting documentation and guidelines on the Intranet.
- Support the reporting process by reviewing incidents jointly with relevant managers.
- Support and facilitate Investigations into incidents as appropriate and following up of serious incidents.
- Ensure that incidents reports to the appropriate persons and/or government agencies.
- Prepare reports for NIPEC's Business Team of all Serious Adverse Incidents and Incidents (as defined in 3.1-3.4) on a regular basis or at least annually as appropriate.
- Ensure records and databases are accurate and up to date.
- Ensure that themes and trends are reported to NIPEC's Health, Safety and Group and other groups such as NIPEC's Information Governance Group and Business Team as appropriate.
- Ensure information on reported incidents is up to date and available for inspection by appropriate persons.
- Ensure escalation of Serious Adverse Incidents (SAIs) to Audit & Risk committee and the Council as appropriate and to keep Sponsor Branch, DoH informed.

2.5 **All staff** are responsible for:

- Reporting any data breach/accident/near miss in line with this policy/procedure.
- Adhering to the employee requirements of the Health & Safety at Work (NI) Order 1978 and associated legislation.
- Applying this policy in regard to information governance issues.
- Provision of reports as requested as part of an investigation.
- Taking appropriate action to ensure incidents do not recur.

3. DEFINITIONS AND CRITERIA

3.1 **An accident** – An unplanned event that causes injury to persons, damage to property or a combination of both and may be minor/ major/ fatal. Injury or harm to staff or other person, caused by an event.

3.2 **An Adverse Incident** – "Any event or circumstances that could have been or did lead to harm, loss or damage to people, property, environment or reputation[1] "which includes an event that has, or may have, impacted upon the delivery of service or health improvement. Incidents include hazards (i.e. anything which has the potential under certain circumstances to cause injury, illness or harm), accidents (direct results of unsafe activities or conditions), dangerous occurrences and significant events. Examples of incidents include:

- Any event that resulted in an adverse effect (however minor) on a service user / member of the public or member of staff
- Failure of equipment, whether or not injury occurs
- Serious damage to property to which NIPEC are tenants
- Serious damage / loss / theft of NIPEC property
- Damage to personal property whilst on NIPEC related business
- Loss / theft of personal property whilst on NIPEC related business
- Fire
- Violence
- Breaches of security
- Lost records/Data Breaches
- Illegal acts
- Breach of Information Governance arrangements.

3.3 **A near miss** - An incident includes near misses. This is where any of the above may have happened had intervention or evasive action not been taken.

3.4 **Serious Adverse Incidents**

- Serious injury to, or the unexpected/unexplained death of:
    - A service user
    - A staff member in the course of their work
    - A member of the public whilst visiting the NIPEC Office.
- Unexpected serious risk to a service user and/or staff member and/or member of the public.
- Unexpected or significant threat to provide service and/or maintain business continuity.

- Serious incidents of public interest or concern relating to:
    - Any of the above criteria
    - Theft, fraud, information breaches or data losses
    - Any incident involving a member of NIPEC staff
    - Other SAIs as defined by Circular HSC (SQSD) 08/2010.

3.5. It is noted that an operational reality for NIPEC is that computer systems fail and that a reporting of each failure would be unnecessarily burdensome. Therefore, as NIPEC's IT service is outsourced to BSO, ITS under a Service Level Agreement (SLA), NIPEC would follow the BSO, ITS procedure which has been put in place.

The ITS system which has been developed is a Dynamic Scoring Index for such issues and this index along with an assessment of criticality of the service based on the Tiered nature of services will guide the need for escalation of the more routine breaks in service. For information an illustration of the tiering of response is as follows:

- **Tier 1** includes Email; Theatre management; ECR; MFDs; Security; OOH; Patient facing Services
- **Tier 2** includes BSTP; Airwatch; Child Health; Business Systems;
- **Tier 3** includes Addiction; Screening; cancer pathways Data warehouse; e-recruitment; FPS systems [1]

In addition to the above the BSO, ITS will produce a quarterly summary of all IT incidents for NIPEC's Business Team's consideration.

4. WHY REPORT AN ADVERSE INCIDENT/ACCIDENT?

4.1 The nature of NIPEC's business involves risks and things can go wrong. By analysing and tackling the root causes of incidents, these risks can be reduced and result in action being taken to reduce the risk of the same or similar incidents occurring.

4.2 There are obligations under legislation and Departmental Guidance to ensure effective management of incidents and accidents. These include:

- Circular HSC (SQSD) 08/2010 covers medical devices, serious equipment failings, fire, counter fraud and security management as well as serious incidents involving staff, service users or members of the public.
- The Social Security Act 1975 requires a person who suffers personal injury by accident whilst at work to notify his employer, manager or supervisor at the time of the accident.
- The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) Health and Safety legislation

[1] These are not exclusive lists but simply an indication of the nature of service

- The Health and Safety at Work Act 1974 and NI Order 1978
- Management of Health and Safety at Work Regulations 1992
- Management of Health and Safety at Work Regulations (Northern Ireland) 2000
- Workplace (Health, Safety and Welfare) Regulations 1992
- Workplace (Health, Safety and Welfare) Regulations (Northern Ireland) 1993
- Manual Handling Operations Regulations 1992 (Amended 2004)
- Provision and Use of Work Equipment Regulations 1998 (PUWER 1998)
- Data Protection Act 1998
- Provision and Use of Work Equipment Regulations (Northern Ireland) 1999Lifting Operations and Lifting Equipment Regulations 1998 (LOLER 1998)
- Lifting Operations and Lifting Equipment Regulations (Northern Ireland) 1999 The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR)
- Human Rights Act 1998
- Disability Discrimination Act 1995
- HSCB guidance on Serious Adverse Incidents as amended from time to time.

4.3 The process of reporting an SAI aims to:

- Focus on service improvement for service users
- Recognise the responsibilities of individual organisations and support them in ensuring compliance
- Clarify the processes relating to the reporting, investigation, dissemination and implementation of learning arising from SAIs which occur during the course of the business of an HSC organisation /Special Agency or commissioned service
- Keep the process for the reporting and review of SAIs under review to ensure it is fit for purpose and minimises unnecessary duplication
- Ensure trends, best practice and learning is identified, disseminated and implemented in a timely manner, in order to prevent recurrence
- Provide a mechanism to effectively share learning in a meaningful way across the HSC
- Maintain a high quality of information and documentation within a time bound process.

5. THE IMMEDIATE MANAGEMENT OF AN INCIDENT

5.1 The immediate responsibility for managing an incident falls to the most senior person on duty at the time the incident occurs. If the event is regarded as a Serious Adverse Incident, the Chief Executive and Head of Corporate Services must be informed immediately and they will decide whether to initiate Business Continuity Plan if required.

5.2 It is the responsibility of the most senior person on duty to:

- Make the situation safe
- Provide or arrange any first aid or medical care as needed
- Decide in conjunction with either the Chief Executive or Head of Corporate Services what other parties require to be informed (taking into account issues of confidentiality), PSNI, NIAS, NIFRS, HSENI, ICO, DoH etc.
- If unable to inform people who need to know, ensure appropriate person(s) are delegated to inform people who need to know, reflective on the nature of the incident
- Ensure that an Incident Report Form has been correctly and fully completed at the earliest opportunity and no later than two working days after the incident
- If the incident relates to a Data Breach, every reasonable effort must be made to locate and retrieve documents lost, altered and disclosed. The Head of Corporate Services will inform the Information Commissioners Office or other relevant body if required
- All communications in regard to a possible Data Breach must be cleared by at least the Head of Corporate Services and the relevant Information Asset officer.

6. REPORTING AND RECORDING SYSTEM

All data breached/accidents and near misses should be reported and investigated as follows:

6.1 All adverse incidents, Accidents and Near Misses must be reported using the NIPEC's Incident Reporting Form (IRF) – see Appendix A

6.2 Forms are available on the NIPEC electronic filing system or from the Head of Corporate Services or Corporate Services Manager

6.3 Forms should be completed and forwarded to the Head of Corporate Services

6.4 Serious Adverse Incidents must be reported to the NIPEC Council and the Sponsor Branch, DoH as soon as possible via the Head of Corporate Services.

6.5 The recording of IT incidents should be logged by email, phone or via Infra (Appendix B). The Assistant Director of BSO's ITS or other relevant Senior Manager will upgrade IT incidents where they fulfil the criteria of 3.4 and in conjunction with the Incident Management Process (Appendix C).

7. RIDDOR REQUIREMENT

7.1 The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) require NIPEC to notify the Health and Safety Executive NI of accidents at work. These reports enable the enforcing authorities to identify where and how risks arise and to investigate serious accidents. It is the responsibility of the Corporate Services Manager to inform the Health &Safety Executive NI, in some instances without delay (e.g. by telephone), of the details of the incident. This must be followed up within ten days with a completed RIDDOR report form, (NI2508).

For further information see the HSENI website http://www.hseni.gov.uk (contains guidelines on RIDDOR).

8. INVESTIGATING AN ADVERSE INCIDENT

8.1 Investigations will be led by someone with the status and knowledge (to make authoritative recommendations and approved by the Senior Management Team. Who investigates an incident will be determined by the nature of the incident, who was involved and where it occurred. A risk adviser, health and safety adviser, managerial or technical staff, or equipment suppliers may need to be involved if events have serious or potentially serious consequences.

8.2 Incident investigations should, if appropriate to the circumstances:

- Identify what happened by obtaining statements/interviewing relevant staff
- Identify how it happened
- Identify why it happened
- Learn from incidents and make recommendations
- Implement improvement strategies to help prevent, or minimize recurrences, thus reducing future risk of harm
- Satisfy mandatory and reporting requirements
- Be carried out using a method called Root Cause Analysis (RCA) (see 9.0)
- A detailed report of the investigation should be compiled.

9. ROOT CAUSE ANALYSIS

9.1 Investigation into Incidents should use Root Cause Analysis methodology. Root Cause Analysis is a structured investigation that aims to identify the true cause of a problem, and the actions that are necessary to either eliminate or significantly reduce the risk.

(Root cause analysis requires the investigator(s) to look beyond the solution to the immediate problem and understand the fundamental or underlying cause(s) of the situation and put them right, thereby preventing re-occurrence of the same issue. This may involve the identification and management of processes, procedures, activities, inactivity, behaviours or conditions.)

10. TRAINING

10.1 Training will be made available, with the assistance of the BSO, for all relevant staff regarding the grading of incidents, completion of incident forms, the SAI reporting process and Root Cause Analysis.

11. MEDIA INVOLVEMENT

11.1 Any media involvement will be handled by the Chief Executive and Head of Corporate Services in association with other relevant senior staff depending on the issue.

12. NIPEC PERFORMANCE AND CONDUCT PROCEDURES

12.1 Whilst the emphasis within NIPEC will be on treating all incidents as a learning experience, a failure to report an incident or an investigation or review of an incident may highlight issues that also need to be dealt with separately under the relevant performance and disciplinary procedures. If such issues arise at any stage with the relevant manager they will be referred to BSO's Human Resource Directorate which will decide whether and when to take any separate action having considered all appropriate options. The investigation of the incident will continue even if a referral to the Human Resource Directorate has been made.

13. EQUALITY SCREENING

The BSO policy from which this NIPEC policy is drawn was screened by BSO Equality Unit. However, NIPEC has also screened this policy.

14. REVIEW

This policy will be reviewed every 3 years or sooner in the event of legislation or regulatory changes, structural or role changes, operational or technological changes, organisational learning, audits and review of the effectiveness of the policy.

Appendix A

Incident Report Form

This form should be completed within

24 Hours

of an incident occurring

To complete the form electronically, first save the form to your desktop. You will notice where you are required to provide text there is a shaded box. This is a protected form and will only allow you to input text in the shaded areas.

Person Involved:		D.O.B.	
Name:		Gender:	☐ Male ☐ Female
Address:			
Postcode:			

Facility Name:		Date of Incident:	
		Time of Incident:	

Witness:

(Please include Name, Department, and/or address and contact number)

Incident Details:

☐ Person

☐ Information

☐ Other

Details of the Incident

Did harm, loss or damage occur?

Please give a brief description of the incident in the Third person only:

(Only state the facts not opinions)*

Immediate Action(s) Taken

- ☐ Notified Line Manager
- ☐ First Aid
- ☐ Ambulance Called
- ☐ Referral to A & E
- ☐ Security/Police
- ☐ Occupational Health
- ☐ Notified Relative

Other Actions Taken:

(Please Specify)

Detail of harm (injury) if apparent:

Other:

(Please Specify)

Body Part(s):

(Please Specify eg, Left Leg etc.)

Degree of Harm (Severity): Choose an item.

Details of Treatment given or Hospitalisation:

If any equipment or furniture is involved it must be taken out of use <u>immediately</u>

Description of Equipment/ Furniture:

Serial No:

Manufacturer:

Item Sent for Repair?

☐ **Yes**

☐ **No**

Item Withdrawn from Use?

☐ **Yes**

☐ **No**

Item Retained for Inspection?

☐ **Yes**

☐ **No**

Reporter Details

Name

Job Title

Phone No

Please forward the form to the Corporate Services Manager. You may also wish to print the form for your own records

Appendix B

Information Technology Services Service Desk

The BSO, ICT Service Desk is open 9:00am to 5:00pm, Monday to Friday except statutory holidays.

If you have an ICT Query or Request, it should be logged through the Infra Service Desk System.

You can do this by either phoning the ITS Service Desk on (028) 9536 2400 or alternatively you may wish to log the details of your Fault or Service Request via the ICT Service Desk Portal. Using the portal you can also monitor progress of your open calls.

Training materials on portal use can be accessed on the links below.

Logging on:

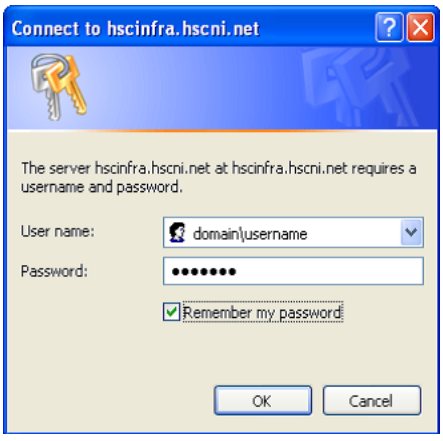
Click on the link to open the portal: ICT Service Desk Portal

You will be required to enter your user ID: e.g. hscni\jbond007.

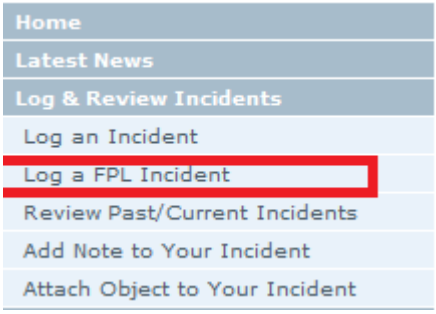
Along with your normal network password.

If you have any problems with the Portal please contact the ICT Service Desk on the number above.

If you place a tick in the Remember my password box, the Portal will log you in automatically in future.



Note: For users of the new Finance Procurement and Logistics (FPL) system, you should now use the option Log a FPL Incident, as shown opposite.



Using this screen from the Infra customer portal will ensure all the relevant information is captured to assist the Service Desk in triaging your FPL calls more efficiently.

What do I need to record on the portal?

The minimum details required:

- Support issue
- Customer's Name
- Location
- Full telephone number
- Asset number of PC / Laptop (sticker on PC / Laptop)
- Your assessment of business impact of the ICT issue
- Details of the ICT issue.

Additional detail to consider:

- Whether other users / PCs have the same issue
- When the system was last working
- If the call is for a password reset, please say what the password reset is for, and provide the username.

Note: The more details that you provide when logging the ICT issue the easier it will be resolved by the BSO, ITS staff.

Appendix C

THE BSO, ICT
INCIDENT MANAGEMENT
PROCESS

1. INTRODUCTION

1.1 Purpose

The objective of the Incident Management process is to restore normal service operations as quickly as possible and minimize the adverse impact on business operations, ensuring that the best possible levels of service quality and availability are maintained.

1.2 Scope

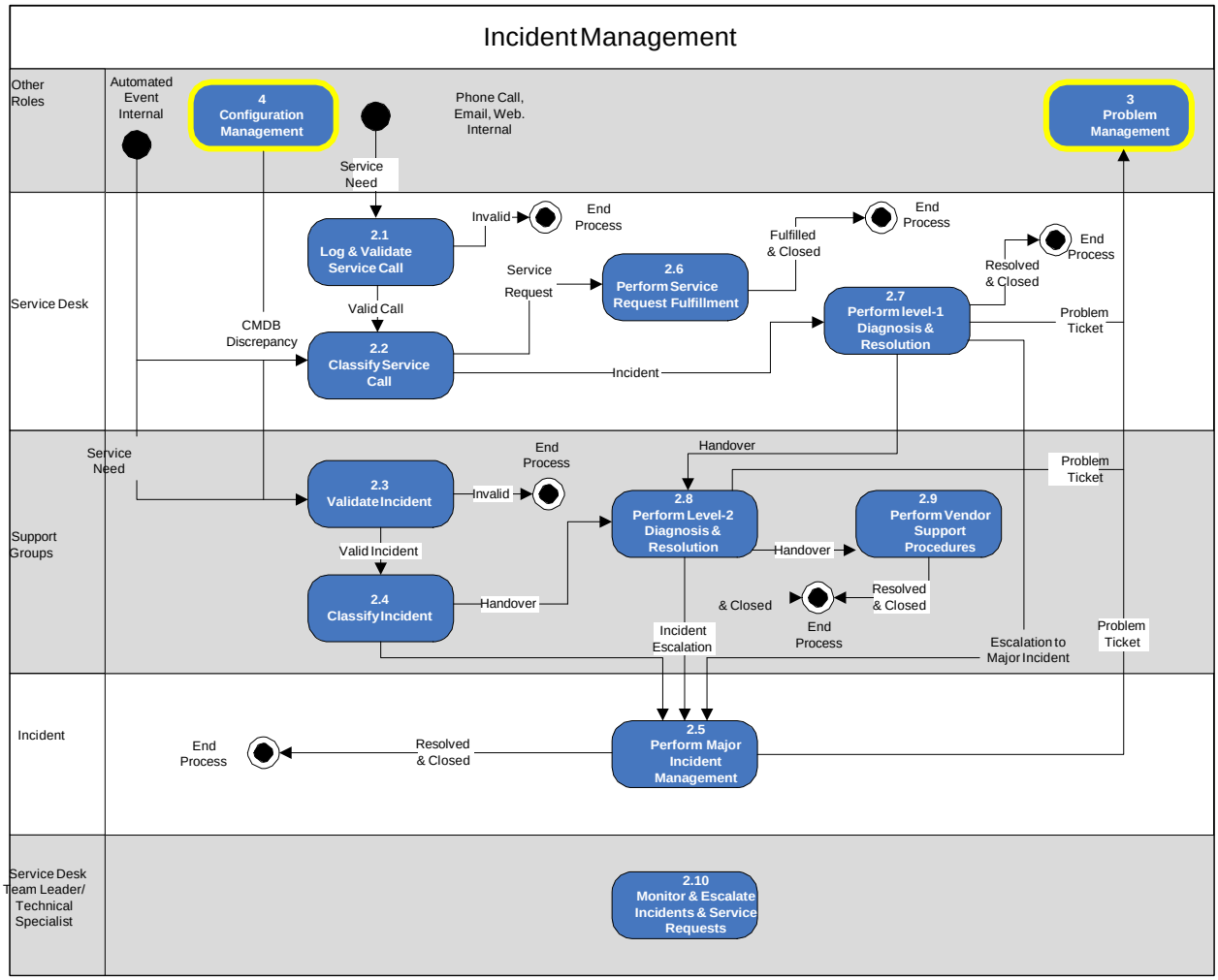
The scope of Incident Management covers all services delivered by and on behalf of BSO ITS to its customers.

1.2.1 This procedure covers:

INCIDENTS	Individual incidences of software, hardware, communications or other operational failure of those products supported by BSO ITS.
SERVICE REQUESTS	Requests for support under the Software Support, Technical Support and Technical System Management services
CUSTOMER FEEDBACK	Cases where a customer complains that a promised service or product was not delivered as agreed. This can be in respect of the timeliness of the delivery of the product or service, or its quality. Also cases where a customer wishes to compliment the service provided. Both complaints and compliments can be in writing, or made verbally during discussions with Product Managers Business Managers, or other personnel engaged in Delivery and Support activities.

2. PROCEDURE

The flow chart below shows how incidents are managed.


Incident Management
Other Roles
Automated Event Internal
4 Configuration Management
Phone Call, Email, Web. Internal
3 Problem Management
Service Need
Service Desk
2.1 Log & Validate Service Call
Invalid
End Process
Fulfilled & Closed
End Process
Resolved & Closed
End Process
Service Request
2.6 Perform Service Request Fulfillment
2.7 Perform level-1 Diagnosis & Resolution
Problem Ticket
Valid Call
CMDB Discrepancy
2.2 Classify Service Call
Incident
Service Need
Support Groups
2.3 Validate Incident
Invalid
End Process
Handover
Problem Ticket
Valid Incident
2.8 Perform Level-2 Diagnosis & Resolution
2.9 Perform Vendor Support Procedures
Handover
2.4 Classify Incident
Handover
& Closed
Resolved & Closed
End Process
Incident Escalation
Escalation to Major Incident
Problem Ticket
Incident
End Process
Resolved & Closed
2.5 Perform Major Incident Management
Service Desk Team Leader/ Technical Specialist
2.10 Monitor & Escalate Incidents & Service Requests

2.1 Incident Escalation

Incidents not resolved within the target times dictated by the agreed priority are escalated through line management as shown in the tables below.

	URGENCY			
IMPACT	Low	Normal	High	Critical
Individual	Low	Medium	Medium	High
Group	Low	Medium	High	High
Facility	Low	Medium	High	Critical
Organisation	Medium	High	Critical	Critical
HSC Service Wide	Medium	High	Critical	Critical

Note: By default all calls have a Priority of Medium, i.e. (Urgency is Normal, Impact is Individual)

PRIORITY	TARGET RESPONSE TIME	TARGET FIX TIME	Infra WARNING e-mail sent to:	ESCALATION			
				SLA Breach	1st escalation	2nd escalation	3rd escalation
			Current Officer & Group	Current Officer & Group	Current Officer & Group	Product / Team Manager	Service Delivery Manager
Critical	1 hour	2 hours	1.5 hours	2 hours	1.5 hours	4 hours	8 hours (1 day)
High	4 hours	8 hours (1 day)	6 hours	8 hours (1 day)	6 hours	16 hours (2 days)	24 hours (3 days)
Medium	8 hours (1 day)	40 hours (1 week)	30 hours	40 hours (1 week)	30 hours	80 hours (2 weeks)	120 hours (3 weeks)
Low	16 hours (2 days)	160 hours (4 weeks)	120 hours (3 weeks)	160 hours (4 weeks)	120 hours (3 weeks)	240 hours (6 weeks)	320 hours (8 weeks)

Note: Once a call breaches its SLA, the call priority cannot be changed.

2.1.2 Level 1 escalations are passed on to the **Current Responsibility Group** at 75% of the target fix time.

2.1.3 Further escalations, according to the Escalation Level, to the Line Manager responsible for the incident's **Current Responsibility Group**.

2.1.4 On receipt of a Level 1 escalation the Current Responsibility Group shall take action to resolve before Target Fix Time.

2.1.5 All escalations are handled automatically by Infra.

2.1.6 On receipt of a Level 2 or Level 3 escalation the Line Manager concerned shall endeavour to discover why the incident remains unresolved. Receipt of the escalation, and detail of the subsequent investigation and its results, shall be recorded against the incident as **Action Text** in the Infra call.

2.1.7 **Level 4** escalations shall be passed to the Assistant Director of ITS in the form of a monthly report listing the relevant incidents as follows :

Priority - Critical:	At end of month in which incident first reported
Priority - High:	At end of month in which incident first reported
Priority - Medium:	At end of month + 1 in which incident first reported
Priority - Low:	At end of month + 2 in which incident first reported

The Assistant Director of ITS shall acknowledge receipt of the report by signing and dating it and shall then request that the Service Delivery Managers provide explanations for late resolution of each incident. The report makes provision for the recording of this information.

2.1.8 Records showing the receipt and subsequent investigation and results shall be retained for no less than three months after successful resolution of the escalated incident.

2.2 Customer Feedback

2.2.1 Customer Complaints shall always be accorded priority **High**.

2.2.2 Any **Customer Complaint** shall be acknowledged in writing to the customer concerned within 2 days of receipt. If resolution of the complaint is also likely within 2 days then this acknowledgement may be combined with the written explanation described in 2.2.3 below.

2.2.3 The resolution of any **Customer Complaint** should include a written explanation of any investigation carried out and any actions taken as a result of the complaint. This should be forwarded to the customer as soon as possible after resolution. The customer will be invited to express either satisfaction or dissatisfaction at the action taken. At this stage the Infra call may be marked as **'Resolved'** but shall normally only be marked as **'Closed'** on receipt of an acknowledgement from the complainant that the action taken was satisfactory. Where there is no response from a complainant after 1 month the incident may be marked as '**Closed**' and an appropriate comment recorded as **Action Text**.

2.2.4 **Customer Compliments** received in writing should be copied to the relevant **Business Manager** and the **Quality Manager** for information. Similarly, customer compliments received verbally should be detailed in an e-mail and copied to the relevant Business Manager and the Quality Manager for information.

3. INCIDENT ANALYSIS

This shall be carried out at three levels

3.1 Service Management Review

3.1.1 A review of any Customer Complaints received during the preceding period shall be carried out as part of the six-monthly **Management Review Meeting** described in the **Management Review** procedure.

3.2 Service Delivery Manager Review

3.2.1 This shall involve a quarterly review of the number of incidents, support requests and complaints logged at Product and Customer level with a view to identifying any shift in the 'norm' that requires further investigation.

3.2.2 This review shall also consider BSO - ITS general performance during the preceding six months in respect of incident resolution times with particular reference to escalation levels.

3.3 Product Manager Review

3.3.1 This shall involve a monthly analysis of the number of incidents and their type logged against the products for which the Product Manager has responsibility. The analysis shall aim to identify unusual fluctuations during the preceding six months and seek explanation for their occurrence. This information can be viewed on SharePoint via the link ‘SLA Performance’.

3.3.2 A second element of incident analysis shall involve the product manager in identifying any repeating incidents or complaints whether they be from the same Customer or from many Customers. This analysis should enable appropriate action to be taken to prevent any unnecessary recurrence of the same or similar incident.